NPS-CAG-14-005

# NAVAL POSTGRADUATE SCHOOL

## MONTEREY, CALIFORNIA

**Trusted Computing Exemplar:
Personnel Security Plan**
by

Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen

12 December 2014

**Prepared for: United States Navy, OPNAV N2/N6**

THIS PAGE INTENTIONALLY LEFT BLANK

**NAVAL POSTGRADUATE SCHOOL**
**Monterey, California 93943-5000**

Ronald A. Route
President

Douglas A. Hensler
Provost

The report entitled “Trusted Computing Exemplar: Personnel Security Plan” was prepared for United States Navy, OPNAV N2/N6 and funded in part by United States Navy, OPNAV N2/N6.

**Further distribution of all or part of this report is authorized.**

**This report was prepared by:**

Paul C. Clark
Research Associate

Cynthia E. Irvine
Distinguished Professor

Thuy D. Nguyen
Research Associate

**Reviewed by:**

Cynthia E. Irvine, Chair
Cyber Academic Group

**Released by:**

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved*<br>OMB No. 0704-0188 |

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| | | |
|---|---|---|
| **1. REPORT DATE** ***(DD-MM-YYYY)***<br>12-12-2014 | **2. REPORT TYPE**<br>Technical Report | **3. DATES COVERED** ***(From-To)***<br>Nov 2013 to Nov 2014 |

| | |
|---|---|
| **4. TITLE AND SUBTITLE**<br>Trusted Computing Exemplar: Personnel Security Plan | **5a. CONTRACT NUMBER** |
| | **5b. GRANT NUMBER** |
| | **5c. PROGRAM ELEMENT NUMBER** |
| **6. AUTHOR(S)**<br>Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen | **5d. PROJECT NUMBER**<br>W4C05 |
| | **5e. TASK NUMBER** |
| | **5f. WORK UNIT NUMBER** |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)**<br>Naval Postgraduate School<br>Monterey, CA 93943-5000 | **8. PERFORMING ORGANIZATION REPORT NUMBER**<br>NPS-CAG-14-005 |
| **9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**<br>Rhonda Onianwa<br>OPNAV, N2N6 F13<br>rhonda.onianwa@navy.mil<br><br>LT David Rivera<br>OPNAV, N2/N6F1<br>david.j.rivera4@navy.mil | **10. SPONSOR/MONITOR'S ACRONYM(S)** |
| | **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** |

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for pubic release; distribution is unlimited

**13. SUPPLEMENTARY NOTES**

The view expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense of the U.S. Government.

**14. ABSTRACT**

This document describes the Life Cycle Management Plan for the development of a high assurance secure product. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

The purpose of this plan is to provide the personnel policy necessary to protect the confidentiality and integrity of a product during the development and maintenance phases of its life cycle. Integrity is the primary concern of this plan, though confidentiality is not disregarded.

**15. SUBJECT TERMS**

Machinery control systems, MCS, life cycle security, high assurance, system security, trustworthy systems

| | | | | | |
|---|---|---|---|---|---|
| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT**<br>UU | **18. NUMBER OF PAGES**<br>19 | **19a. NAME OF RESPONSIBLE PERSON**<br>Cynthia E. Irvine |
| **a. REPORT**<br>Unclassified | **b. ABSTRACT**<br>Unclassified | **c. THIS PAGE**<br>Unclassified | | | **19b. TELEPHONE NUMBER** ***(include area code)***<br>(831) 656 2461 |

THIS PAGE INTENTIONALLY LEFT BLANK

CYBER ACADEMIC GROUP
NAVAL POSTGRADUATE SCHOOL

NPS-CAG-14-005

# Trusted Computing Exemplar: Personnel Security Plan

Paul C. Clark
Cynthia E. Irvine
Thuy D. Nguyen

December 2014

## ATTRIBUTION REQUEST

December 2014

The Cyber Academic Group (CAG) and the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) wish to facilitate and encourage the development of highly robust security systems.

To further this goal, the NPS CAG and NPS CISR ask that any derivative products, code, writings, and/or other derivative materials, include an attribution for NPS CAG and NPS CISR. This is to ensure that the public has a full opportunity to direct questions about the nature and functioning of the source materials to the original creators.

## ACKNOWLEDGEMENT

The authors gratefully acknowledge the following organizations for providing support toward the development of this work: OPNAV N2/N6 F1.

The material presented here builds upon work supported in previous years by the Office of Naval Research.

A portion of the material presented here is based upon work supported by the National Science Foundation under Grant No. CNS-0430566 and CNS-0430598. This document does not necessarily reflect the views of the National Science Foundation.

# Table of Contents

# Table of Figures

# 1 Introduction

This document has been written in support of a research project to publicly demonstrate and document how a high assurance product can be developed and distributed. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

The purpose of this plan is to provide the personnel policy necessary to protect the confidentiality and integrity of a product during the development and maintenance phases of its life cycle. Integrity is the primary concern of this plan, though confidentiality is not disregarded.

# 2 Policy

This section defines the policy with respect to personnel security, as it applies to the TCX project.

1. Specific qualifications for participation on a project (e.g., clearances, U.S. citizenship, DoD employee, etc.) are set by the Project Manager based on the needs of the individual aspects of the project (such as the projected customer base), and not as a requirement for high assurance.

2. A new user shall be promptly trained.

   A new user (viz., a new participant on a project) shall be familiarized with the security requirements of the project, and trained on the proper use of the development or CM systems, before access is given to the systems. The Project Manager shall maintain evidence of this training. Training shall consist of reading the internal documents that apply to the user's responsibilities, as determined by the Project Manager. For example, a developer may be assigned to read the following documents:
   a. Physical Security Plan
   b. Personnel Security Plan
   c. Development Standards
   d. Configuration Management Procedures

   Evidence of this training shall include the new user's signature indicating that the documents have been read, that they have been understood, and that the user agrees to abide by them. (See Appendix A).

3. Refresher training shall be performed annually.

All personnel involved on a project shall have a yearly refresher of the associated security requirements. The Project Manager shall maintain evidence of this training.

4. A user shall be considered authorized to access project systems after approval has been given by the Project Manager, and after training has been completed.

5. An official list of authorized users shall be maintained.

   The Project Manager shall maintain two lists of authorized users:
   a. Those authorized to access CM systems. (See Appendix C).
   b. Those authorized to access development systems. (See Appendix B).

   Each list shall show the full name of the user, the login name of the user, the Discretionary Access Control (DAC) groups the user is assigned to, and the date approval was given.

6. No user shall be allowed on both lists of authorized users.

   The CM systems and the development systems shall have two separate system administrators.

7. A system administrator shall not add or disable accounts without direction from the Project Manager.

8. When a user separates from a project, the Project Manager shall update the list of authorized users and direct the system administrator to disable the respective account.

9. The accounts of separated users shall be disabled promptly.

   When informed by the Project Manager of a separated user, the system administrator for the respective account shall promptly disable it. Confirmation of this action shall be communicated to the Project Manager, who shall note the date on the list of authorized users.

10. If a separating user is a system administrator, then the administrative password(s) shall be changed immediately.

    If a new system administrator has not been identified at the time of separation, the Project Manager shall maintain the new password until a replacement has been appointed.

11. When a user separates from a project, all evaluation evidence and other project material maintained by that user shall be turned over to the Project Manager.

12. Audits shall be performed at least quarterly.

    The Project Manager is responsible for verifying that all enabled accounts of the systems are on the appropriate list of authorized users.

    Evidence of these audits, and their results, shall be kept by the Project Manager. (See Appendix D).

# 3 Responsibilities

This section assigns responsibility for meeting the requirements of this document.

1. Project Manager

   The Project Manager is responsible for selecting personnel to work on a project, and ensuring that they are properly trained. The Project Manager must maintain accurate lists of authorized users, notifying the system administrators in a timely fashion when changes have been made, and conducting regular audits of the lists.

2. System Administrators

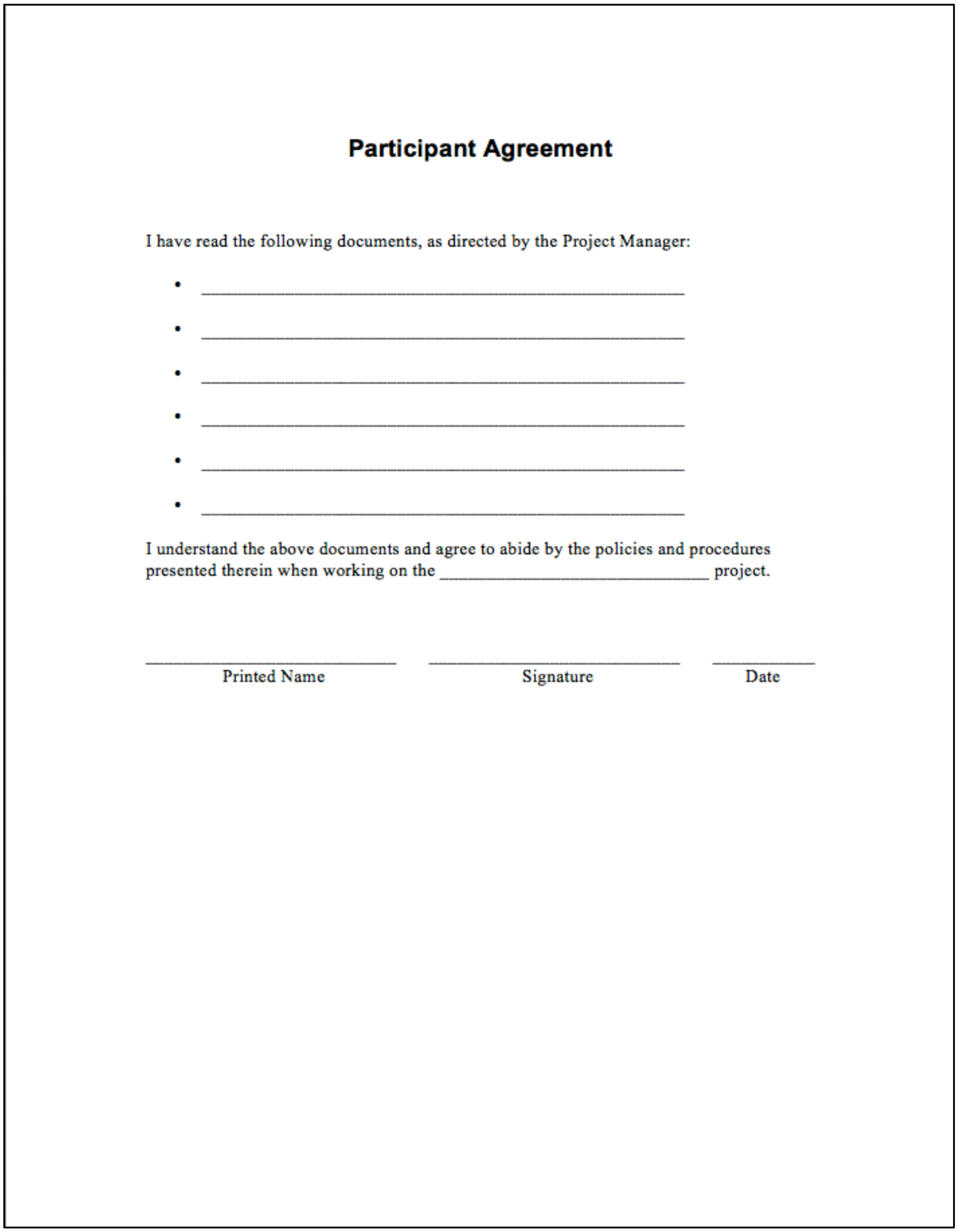
   The system administrators must follow the direction of the Project Manager by either adding or disabling user accounts upon request.

3. All Project members

   All members of a project must comply with the personnel policies, as stated in this document. The whole team can help the Project Manager, especially the Configuration Item Leaders, to keep track of personnel as they leave, which can be a challenge in some environments.

# Appendix A – Participant Agreement

Figure 1 shows an example of an agreement that a project member is required to sign, showing evidence of initial training and a willingness to abide by the policies set forth by the project.



## Participant Agreement

I have read the following documents, as directed by the Project Manager:

- ______________________________________________
- ______________________________________________
- ______________________________________________
- ______________________________________________
- ______________________________________________
- ______________________________________________

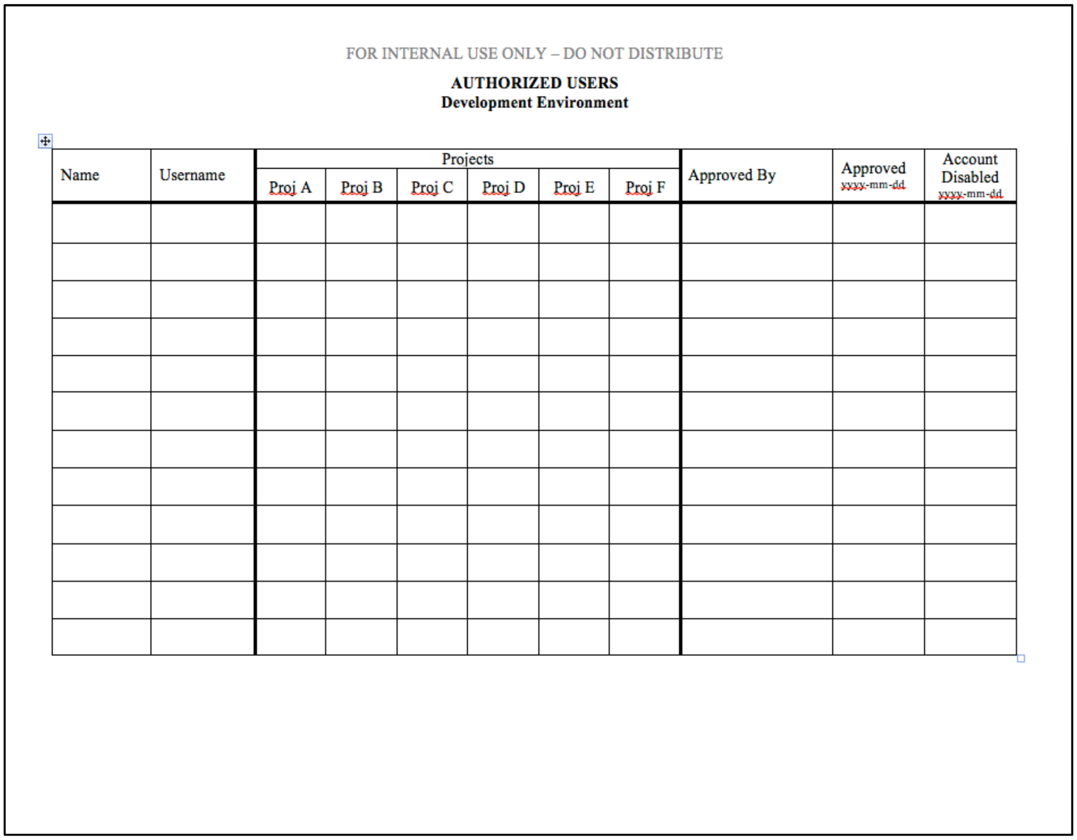
I understand the above documents and agree to abide by the policies and procedures presented therein when working on the __________________________ project.

| | | |
|---|---|---|
| ________________________ | ________________________ | __________ |
| Printed Name | Signature | Date |

**Figure 1 Sample Participant Agreement**

# Appendix B – Authorized Users on Development Systems

Figure 2 shows a sample record to keep track of authorized developers, per project.



FOR INTERNAL USE ONLY – DO NOT DISTRIBUTE

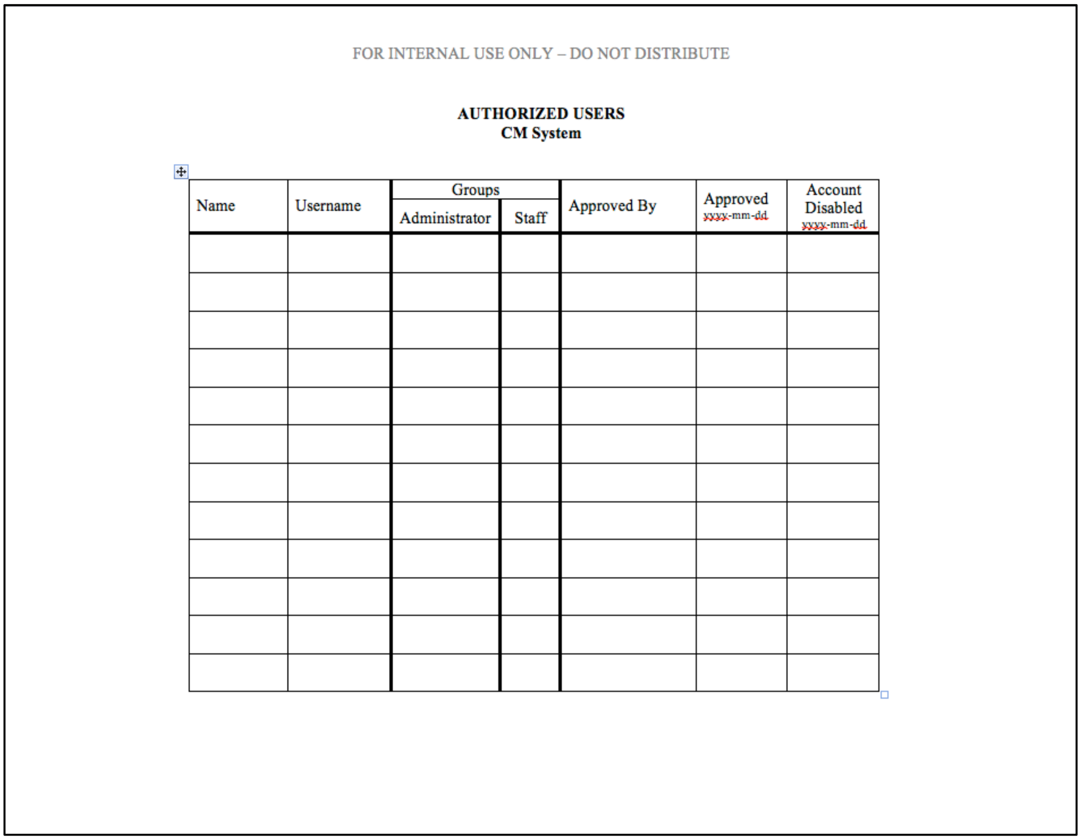
**AUTHORIZED USERS**
**Development Environment**

| Name | Username | Projects | | | | | | Approved By | Approved<br>yyyy-mm-dd | Account Disabled<br>yyyy-mm-dd |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Proj A | Proj B | Proj C | Proj D | Proj E | Proj F | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

**Figure 2 Sample Record of Authorized Users on Development Systems**

# Appendix C – Authorized Users on CM Systems

Figure 3 shows a sample record to keep track of authorized users on the CM system.



FOR INTERNAL USE ONLY – DO NOT DISTRIBUTE

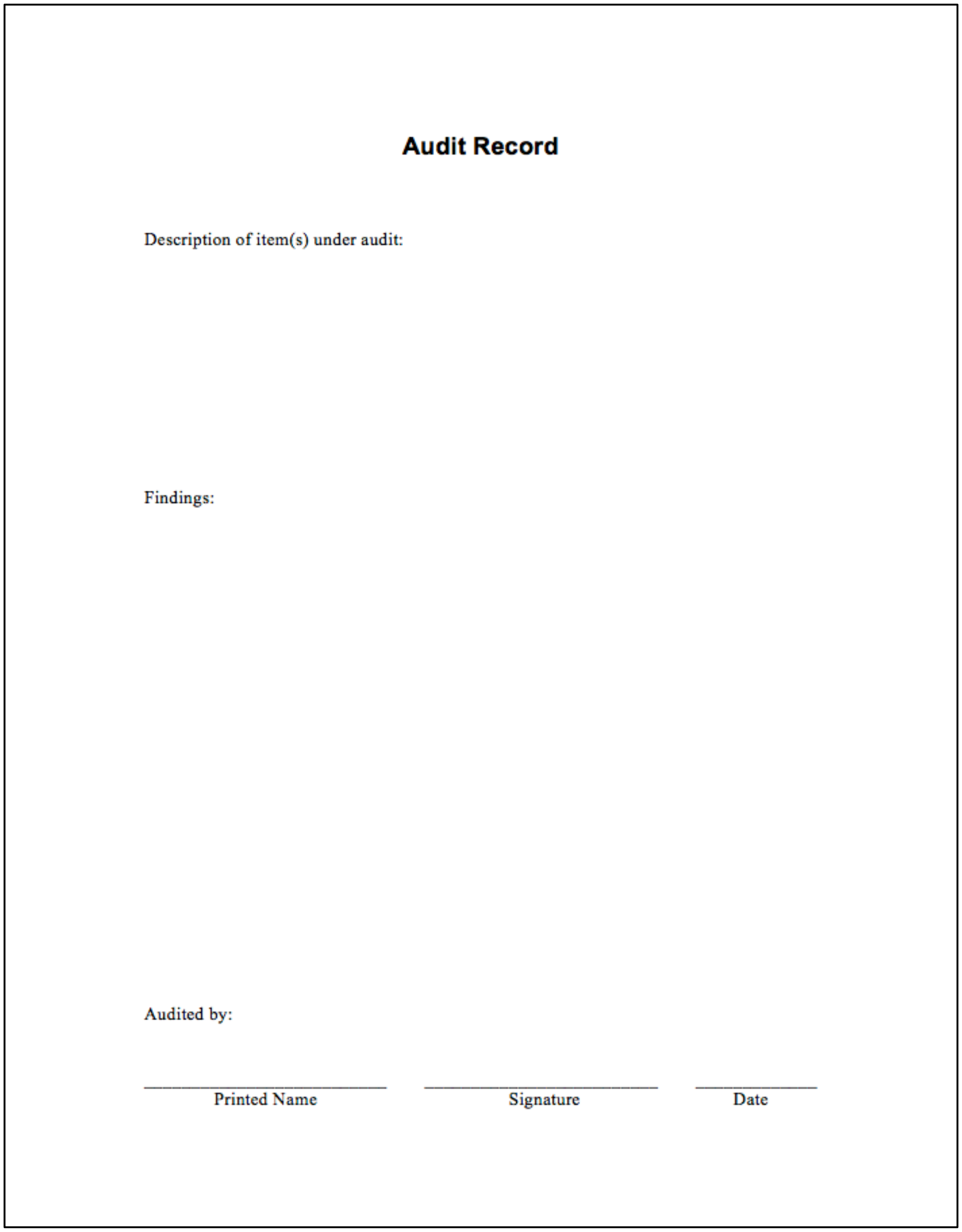
**AUTHORIZED USERS**
**CM System**

| Name | Username | Groups | | Approved By | Approved<br>yyyy-mm-dd | Account Disabled<br>yyyy-mm-dd |
|---|---|---|---|---|---|---|
| | | Administrator | Staff | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Figure 3 Sample Record of Authorized Users on the CM System**

# Appendix D – Audit Records

Figure 4 shows a sample record to provide evidence that audits were performed as required.



**Audit Record**

Description of item(s) under audit:

Findings:

Audited by:

__________________________ _________________________ _____________
Printed Name Signature Date

**Figure 4 Sample Audit Record**

[THIS PAGE IS INTENTIONALLY BLANK]

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Ft. Belvoir, Virginia

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School
   Monterey, California 93943

3. Research Sponsored Programs Office, Code 41 1
   Naval Postgraduate School
   Monterey, California 93943

4. Paul C. Clark 1
   Naval Postgraduate School
   Monterey, California 93943

5. Dr. Cynthia E. Irvine 1
   Naval Postgraduate School
   Monterey, California 93943

6. Thuy D. Nguyen 1
   Naval Postgraduate School
   Monterey, California 93943